GN Docket Nos. 09-47, 09-51, and 09-137
"Comments—NBP Public Notice #20"

Voting is the most fundamental of civic acts. As technology transforms all aspects of society, could voting be transformed as well?

a. With existing technology, is it possible to enable and ensure safe and secure voting online today?

Online voting is the casting of votes by electronic means rather than traditional means such as paper ballots or postal ballots. It is already used in many countries all over the world. While some countries carried out only pilot voting projects to test the new technology, in other countries electronic voting is part of the normal voting process.

Countries with recent experiences in online voting are France, Finland, Austria, Switzerland, Australia and Estonia. Also in the United States a very important online voting project was carried out – the 2008 Presidential election in Okaloosa County, Florida.

As electronic voting can help improving current electoral systems, the Organization of American States (OAS)[1] and the Council of Europe[2], have established standards and guidelines on how to implement online voting in a secure and reliable manner.

Electronic voting presents numerous advantages over traditional paper-based voting. Several key advantages are: The speed and accuracy in the vote counting process; online voting offers better accessibility for blind and visually impaired people; the flexibility in the design and modification of the ballots is easier; it prevents of involuntary voting errors (e.g., "over-voting" and "under-voting" errors) as well as the support of multiple languages. In addition online voting offers the further advantage of voters' mobility and convenience which generally leads to higher participation rates.

Conducting an electronic election that involves ballots in digital form is a complex issue that raises a number of security concerns. The confidence relationships found in traditional elections must be

[1] See here also the recommendations from the United States Election Assistance Commission http://www.eac.gov/voting%20systems/voting-system-certification/2005-vvsg

[2] http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf

replicated in electronic systems, without losing reliability. Electronic voting must therefore reproduce the practices of traditional voting methods (e.g. secure identification of voters, as well as distribution of trust among the members of an Electoral Board). Additionally, electronic voting faces new requirements (e.g. new privileged actors such as system administrators) and new technical risks (e.g. digital ballot formats that are more easily manipulated than physical ones).

Digital security measures are therefore paramount for electronic voting success. However, conventional computer and network security measures (e.g. firewalls, intrusion detection systems, antivirus software...) fall short of providing a complete solution to electronic voting. These generic security measures, although regularly used to secure e-commerce and e-business transactions, are not enough for e-voting. Indeed, casting ballots is not an ordinary transaction. When performed electronically, it must address the following requirements and security concerns:

- **Authenticity of ballots**: Reliable means to verify the origin of a ballot (i.e. the identity of the voter that casts it) must be used to ensure the “one voter, one vote” premise.
- **Privacy of voters**: Despite the previous requirement, it must be impossible to correlate the votes to the identities of their respective voters, unless required by law (as it is in some countries).
- **Accuracy of election results**: It must not be possible for anyone to remove or alter the ballots that have been cast by eligible voters or to add invalid ballots (e.g. on behalf of abstaining voters).
- **Secrecy of intermediate results**: To ensure that voters’ choices are unbiased, intermediate results must be secret until the election is completed.
- **Ballot verifiability**: Voters must be able to independently verify that their ballots have been correctly accounted for.
- **Uncoercibility**: The fact that voters are allowed to verify their votes must not make some fraudulent practices such as coercion or vote-selling possible

The digital security measures for e-voting must meet the previous list of requirements, detecting and preventing fraudulent practices even when they are performed by privileged actors in electronic voting environments (e.g. electoral authorities or systems administrators). There is only one way to ensure the fulfillment of these security requirements that are specific to e-voting applications, and therefore to ensure reliability of electronic voting systems: to construct digital security measures around an application-level cryptographic e-voting framework.

Cryptographic e-voting protocol proposals allow achieving these before mentioned security requirements. For this reason, online voting is already now more secure and efficient compared to postal voting.

More information can be found in http://scytl.com/_a_home/PNYXCOREWhitePaper.pdf

b. What can we learn from other nations that have considered or implemented online voting?

Electronic voting was implemented in many countries during the last years. Different experiences were gained in pilot projects all over the world.

Usually governments start implementing the new online voting channel with pilot projects. First they allow the casting of votes only to a limited and privileged amount of people. This first step helps to analyze the technology and also the acceptance of the citizens. The first possible voters with the permission to vote with the new online voting technology could be absentee voters or military personnel. They are often more open to the new voting channel, as they suffer different constraints when casting votes (paper ballots are received too late, voting from abroad not allowed, etc).
After sufficient experiences were gained and the new voting technology has facilitated the casting of the votes, governments usually allow in a second step electronic voting to other (all) citizens.

Below you find a list of countries that have tested electronic voting as described above and gained their experiences.

In the US, the **County of Okaloosa, Florida**, wanted to give their military personnel the possibility to securely cast votes over the internet. Therefore, in 2007, the Secretary of State of Florida approved a project that allowed for the first time U.S. citizens to cast votes remotely from designated voting terminals in a U.S Presidential election. Okaloosa County is the county with the highest concentration of active duty military deployed around the world. The objective of the State of Florida was to address the difficulties that the State's overseas citizens encounter when it comes to participating in the country's electoral processes. This first online voting election can also be seen as test for future implementation for more elections. (Detailed information also under http://scytl.com/_a_customers/USA_eng.pdf)

Switzerland is a good example of the description provided above. In Switzerland 3 cantons carried out electronic voting as a first pilot project. In Zürich, Neuchatel (information to the project available in French only under http://www.ne.ch/) and Geneva electronic voting was offered in several elections and referendums to a limited amount of citizens. The technical aspects and the acceptance of the citizens were analyzed. On the experiences gained, the Swiss government decided to introduce electronic voting for the whole country. Now, also other cantons join the e-voting project.

Another country that has carried out several pilot projects is **France**. In 2009 the French government enabled their citizens living abroad to cast electronically their ballots for their representatives in the French senate. This project went technically well and therefore the French Government will use the new voting channel also in other elections. (More information to the project http://scytl.com/_a_customers/France_eng.pdf)

Austria used an electronic voting system for binding elections for the first time in 2009. Tests were carried out already in the past but the students elections 2009 for all Austrian public universities was one of the most important modernization projects in Austria.

Estonia is also a country that has a very high acceptance of online voting. Already in 2002 Estonia created the legal basis for electronic voting.[3] Now electronic elections are accepted as much as the traditional paper based election. Before introducing electronic voting, all parties in Estonia agreed on a fairness agreement: this meant that parties would not organize collective voting actions; they will never send e-campaign materials with a link to the e-voting website and threaten without objective reasons the legitimacy of elections and e-voting on selfish day politics grounds. For the Estonian government electronic voting is a very important and prestigious project. (http://www.vvk.ee/?lang=en)

Here it is also important to mention the experience made in **Catalonia** (a northern region in Spain) in their 2003 Catalonian parliament elections. The evaluation of the project showed, that the online voting channel is a more **secure channel** compared to the postal voting channel where votes often are lost. This problem is due to ineffectiveness in the postal service, such as the delay in delivering the ballots, the transportation of blank ballots from the election official to voters or the transportation of returned voted ballots.

Another aspect that creates trust in the new voting technology is the **audit** of the electronic voting system before it is used during the election. The audit should always be carried out by independent experts in security before the implementation is carried out. The selection of these experts should be done by the institution that decides to carry out the online voting project. An audit creates trust in the implemented system, always under the condition, that it is carried out by independent experts and that the results are published.

[3] The different Estonian laws regarding elections can be found under http://www.vvk.ee/index.php?id=11155

All the before mentioned experiences and results can help each country when thinking about the implementation of a new online voting channel.

c. What can we learn from pilot projects that have tested online voting?

See the answer provided in point b.

d. Have localities or states enabled online voting either domestically or for citizens abroad (such as military personnel stationed overseas)?

Different online voting projects were carried out in the US during the last years. As described already in question b.), online voting can be seen as a development process. Tests can be carried out for special privileged citizens (absentee voters, military personnel etc.) or also on different geographical levels. There test can be carried out on local, county or state level.

The most important online project in the US was carried out in **Florida** – **Okaloosa County** (**http://www.dos.state.fl.us/**). To allow online voting for the U.S Presidential elections in 2008, the Secretary of State of Florida approved in 2007 the project that allowed for the first time U.S. citizens to cast votes remotely from designated voting terminals in a U.S Presidential election.

Okaloosa County was chosen as it is Florida's county with the highest concentration of active duty military deployed around the world. In order to carry out this project Scytl's secure e-voting technology Pnyx was chosen. Pnyx, is the first and only Internet Voting solution certified in the US. It was certified by the Florida Department of State, Division of Elections. In polling places in England, Germany and Japan it allowed US citizens living abroad to cast electronic ballots during several days. Each polling station was equipped with several voting terminals (a conventional laptop plus a printer, touch screen and smartcard reader). A central electoral board located in Florida was in charge of reviewing the received and, once the election was closed, of decrypting the valid ballots and obtaining the final results.

The objective of the State of Florida was to address the difficulties that the State's overseas citizens encounter when it comes to participating in the country's electoral processes. This objective was reached and this online voting project can be seen as the most important online voting project in the US.

e. Do government jurisdictions at any level, domestic or foreign, allow online voting for any citizen? Have there been quantifiable impacts tied to online voting, including impacts on the number of citizens that voted? Have there been qualitative impacts tied to online voting, either positive or negative?

The question above consists of 3 questions which are answered below.

Online voting is permitted in different countries worldwide. There are even countries that carry out electronic elections continuously. France and Switzerland allow electronic voting for their citizens, Austria tested electronic voting for their university students, Estonia uses electronic voting for their voting process with high acceptance, in Florida a pilot was carried out permitting military personnel to vote for the presidential elections 2008, the Netherlands, Finland made their experience and also Australia and Philippines have carried out online voting projects. In addition, enabling legislation was passed in Colorado in 2009 to allow for pilot testing online voting technology; Alabama, Washington, Georgia and Hawaii are expected to pass legislation early in their respective 2010 sessions.

Different databases exist that give an overview over existing online voting projects. One of the most important is e-voting.cc which gives an overview on all worldwide projects that were carried out. E-Voting.cc offers also a very interesting study of the e-voting readiness of most European countries and the US (http://www.e-voting.cc/static/evoting/files/krimmer_schuster_wp_01_2008-pdf.pdf). The interesting aspect of this study is not only, that it gives information about the readiness regarding electronic voting of states but also analyses the legal framework of each country.

It is discussed whether electronic voting augments the turnout of voters or not. It is certain, that electronic voting facilitates the casting of votes for many people. It is certain, that the costs for elections diminish when using electronic voting for a bigger electoral roll. In Switzerland it was noticed, that in some elections the turnout through the online voting channel was higher than the turnout of the paper channel. ((http://www.geneve.ch/evoting/rapports_20041128.asp).

The qualitative impacts can be especially seen in the turnout rates. Many countries that permitted electronic voting have higher voter turnouts. Another positive impact is the better accessibility. (Regarding the accessibility also see http://www.evoting.cc/static/evoting/files/barrat_a_preliminary_question_51-60.pdf)

f. What are the security and privacy risks that government jurisdictions must consider when considering the implementation of online voting?

Electronic elections must be at least as safe as traditional paper elections. In electronic voting you can normally find actors with special privileges. These could be system administrators or any other actors with privileges.

Therefore an electronic voting solution needs to provide end-to-end security. This means, that the vote is protected from the individual voter to the Electoral Board. This is also a secure measure that prevents from internal attacks made by system administrators.

To achieve this goal special security requirements must be taken into consideration: votes are encrypted and digitally signed by voters in the voters' voting devices (e.g., PCs) before they are cast. The private key to decrypt the votes is divided in shares and these shares are distributed to the Electoral Board members before the election begins. The private key is destroyed in this splitting process and, therefore, does not exist during the election. At the end of the election, a pre-defined minimum number of Electoral Board members have to meet to reconstruct the private key and decrypt the votes.

An Internet voting solution shall always put the control of the electoral process in the hands of the Electoral Board. This is also the case in the traditional paper-based election. The Electoral Board members shall always be the only ones that can reconstruct the key to decrypt and count the votes.

System administrators or any other actors with privileges in the system do not have access to the private key and, therefore, cannot see nor modify clear-text votes.

More information is also available under http://scytl.com/producto_ing_8_20_49.htm.

g. What are the history and current state of play of online voting technologies?

Online voting projects were carried out all over the world during the last years. Many nations tested the implementation of this new technology and made different experiences. Below we can mention only some of these projects and explain the online voting technology. Also different technologies were used in their projects.

Estonia: Internet voting with binding results has been carried out twice in political elections: in local elections of October 2005 and parliamentary elections of March 2007. Therefore also the Estonian legislation needed to be adapted to the new voting technology.

France: The French Ministry of Foreign Affairs has selected Scytl to offer a 24/7 secure Internet voting platform to the French citizens living overseas. In May 2009, 340.000 French voters residing in Africa and America were able to cast votes over the Internet to elect their representatives to the Assembly of the French living abroad (AFE). The AFE elected directly 12 Senators who represent the French living overseas. This was the highest-profile internet voting project in France.

Switzerland: in Switzerland the main pilots of e-Voting in Neuchatel, Zurich and Geneva. The 3 different cantons have all different solution providers. The Swiss project started already in 1998, when the federal executive has launched a governmental project. The idea was to enable the exercise of political right also by an online channel. As a next step the Swiss government has plans to give the possibility to use this voting channel for the whole country.

In the **USA, Florida** a pilot project for military personnel was carried out. This was also a successful test to use the electronic voting channel for future elections.

Austria: the Austrian Ministry of Science and Research allowed their students to cast votes for their representatives over the Internet. There a voting project was carried out for all university students. This can be seen as a first step to introduce electronic voting also on a national level.

UK: also in the United Kingdom tests with electronic voting were carried out. In 2006, the Ministry of Justice of the United Kingdom made several tests in the whole country within their 4-year Electoral Modernization Program. Citizens in different districts were allowed to securely cast binding votes remotely over the Internet during their May 2007 local elections. Paper-based voting and postal-voting were also valid voting channels, used in parallel to the electronic one. The results have been very positive, including several soldiers voting from different countries.

Canada: another country were increasing experiences in the online voting can be seen is Canada. Since the 90s it was used at the municipal level in some cities.[4]

h. What are best practice processes concerning online voting?

When implementing a new voting technology, the technology needs to fulfill several requirements. First of all the technology must be recognized and internationally already been used. This creates trust among voters. The implemented voting solution also needs to be audited and after the **audit** process

[4] http://www.peterboroughvotes.ca/internet.shtml

the solution needs to be **certified**. Audit or certification shall always be done by an independent institution appointed by the election authorities.

Before the technology is successfully implemented, the governmental institution must think of which group of people shall be the ones testing for the first time the new voting channel. These can be absentee voters, military personnel or students at universities.

Besides the before mentioned information, also security aspects need to be taken into consideration. Different measures are implemented that bring online voting to the highest possible standard. Highest security standards are ensured by the Shamir secret sharing scheme, the immutable logs, mixing and the vote verification:

In order to protect voter privacy the submitted ballots should be encrypted using a public key, associated with a secret key that is needed to decrypt them. This secret key, generated at the election configuration stage, can be split into several secret shares using a **Shamir Secret Sharing Scheme** and distributed among the Electoral Board members to enhance the system security. The Shamir Secret Sharing Scheme can be configured with a threshold parameter, in such a way that a qualified majority of members of the Electoral Board must then provide their secret shares in order to reconstruct the private key and allow the decryption of the encrypted ballots. Therefore, the private key does not exist until the voting process has finished and cannot be compromised by any privileged actors.

Mixing is a security standard that also ensures reliable elections. The main goal of the mixing protocol is to ensure that the ballots are properly decrypted and taken into account, without compromising the privacy of voters. The correlation between each voter and his/her vote is separated. Ballot mixing can proceed only when a private key, associated with the public key used to seal the inner digital envelopes, is reconstructed at the mixing server. During the election configuration, this key was split into several secret shares and distributed among the Electoral Board members. A qualified majority of members of the Electoral Board must provide their secret shares in order to reconstruct the private key and allow the opening of digital envelopes. To enhance the security of the process, these shares may be stored in personal cryptographic devices (such as smartcards).

In order to allow the verification of the election integrity by authorized auditors, the election components must save logs that register all their important operations. For example, the voting servers can store the time of reception of each request, the stored encrypted ballots, etc. Thus, if someone erases any critical information it can be detected through the logs. These logs have to be protected from deletion or manipulation, and allow checking of their integrity by third parties. To this end, **Immutable Logs** should be used, where each time a new log is created it is chained to the previous log and digitally signed. Therefore, if anyone tries to delete a log, the posterior logs chained to it allow the detection of this deletion, and if anyone tries to forge a false log, the digital signature on it will not be correct.

Another security measures that creates trust is the **vote verification**: it creates security among citizens because it gives the voter the possibility to verify if the vote has been counted by the electoral commission. A few examples may serve to illustrate the effectiveness of individual verifiability to detect general manipulations of the election results: In an election with 2,000 ballots cast, only 30 voters are required to verify the presence of their own ballots on the tabulated results in order to achieve a more than 90% probability to detect a manipulation of just 150 ballots. If the number of voters that verify doubles (that is, just 60 voters), the probability of detection rises to more than 99%. In an election with 40,000 ballots cast and a manipulation of just 1% of them, the chances of detecting the manipulation are more than 90% if just 230 voters verify. If 2% of the voters verify their ballots, the same manipulation is detected with a probability of more than 99.9%.

The before mentioned security measures are necessary to ensure the highest standard of electronic voting.

i. How would enabling online voting impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas?

The impact of overseas military personnel, overseas diplomatic personnel and other Americans living overseas would be positive. While traditional postal mail has been the mainstay of overseas voting to date, it is fraught with inherent challenges: Reliance of country of location postal services, remote nature of personnel in areas under-served by postal services, and the transient nature in particular of overseas military personnel to cite only a few examples. While online voting may not be accessible in all locations, as is the case with postal services, it provides one additional path for overseas voters to use: A path that can expedite the process of ballot delivery and subsequent return of voted ballots in time for inclusion in election tally.

Significant portions of the globe are wired for internet connection (wired/not wired). In particular military personnel in forward deployed combat environments have access in many instances to internet connection. Online voting while not the total answer for overseas voting challenges, it does represent a relatively inexpensive additional channel for this voter group to utilize successfully.